



# **ANLAGE 17**

## **INFORMATIONSSICHERHEITSRICHTLINIEN**

November 2024

Dieses Dokument enthält firmeneigene Informationen der MAN Truck & Bus. Dieses Dokument und die darin enthaltenen Informationen dürfen nur mit ausdrücklicher vorheriger schriftlicher Zustimmung der MAN Truck & Bus veröffentlicht, weitergegeben oder zu anderen Zwecken eingesetzt werden.

## Richtlinien für den Anbieter

Dieses Dokument enthält spezifische Informationen, die MAN den Anbietern für die Beantwortung der Ausschreibung zur Verfügung stellt.

## Anweisungen für den Anbieter

1. Der Anbieter verpflichtet sich, keine Änderungen oder Modifikationen an diesem Dokument vorzunehmen.
2. Die Antwort des Anbieters auf diese Ausschreibung sollte die Informationen in diesem Dokument widerspiegeln und diesen Angaben entsprechen.
3. Einwände oder Probleme in Verbindung mit den in den Dokumenten enthaltenen Definitionen machen die Anforderungen dieses Dokuments oder der Ausschreibung weder ungültig noch bewirken sie eine Modifizierung der Anforderungen. Von einer Aufnahme der vorgeschlagenen Änderungen des Anbieters kann der Anbieter nur ausgehen, sofern die MAN diese dem Anbieter gegenüber ausdrücklich schriftlich bestätigt hat.

Ref #	
Anl. 17 - 1	<b>ÜBERBLICK</b>
Anl. 17 - 2	Gesetzliche Regelungen fordern für sensible Unternehmenswerte „Sicherheitsmaßnahmen“, die zur Aufrechterhaltung des Geschäftsbetriebs einer Organisation von entscheidender Wichtigkeit sind. Mit wachsender Digitalisierung sind zu schützende „Informationswerte“ zunehmenden „Bedrohungen“ ausgesetzt. Systeme, deren Funktionen, Netze und Organisationen sind gefährdet durch <i>Cyber-Angriffe</i> (Schadsoftware, Hacking, Denial-of-Service-Angriffe, Phishing etc.), Sabotage, Spionage und Vandalismus, aber auch Elementarschäden durch Wasser, Feuer, Katastrophen und andere „Gefahren“.
Anl. 17 - 3	Ziel des Managements von Informationssicherheit, ist es ein angemessenes Informationssicherheitsniveau der MAN zu bewahren. Hierzu ist im Informationssicherheitsmanagementsystem (ISMS) ein Sicherheitsregelwerk (Security Policies) definiert, das die Einhaltung von unternehmensinternen, normativen und gesetzlichen Anforderungen fordert.
Anl. 17 - 4	Die primären Schutzziele für die „Informationswerte“ der MAN sind „Vertraulichkeit“, „Integrität“, „Verfügbarkeit“ (engl. Confidentiality, Integrity and Availability). Die erweiterten Schutzziele sind Authentizität, „Zurechenbarkeit“, „Nicht-Abstreitbarkeit“ und „Verlässlichkeit“ (engl. Authenticity, Accountability, Non-Repudiation and Reliability).
Anl. 17 - 5	Der AN wird die Geschäftsbeziehung mit MAN sowie sämtliche im Rahmen dieser Geschäftsbeziehung ausgetauschten Informationen streng geheim halten. Er verpflichtet sich diese Informationen gemäß diesen zur Verfügung gestellten Informationssicherheitsrichtlinien der MAN, mittels geeigneter Maßnahmen vor Dritten sorgfältig zu schützen. Die Geheimhaltungspflicht gilt nach Beendigung oder vollständiger Abwicklung der jeweiligen Beauftragung für einen Zeitraum gem. IT-AEB weiter. Die Geheimhaltungsverpflichtung gilt unabhängig von einem Vertragsabschluss auch für in der Angebotsphase erlangte Kenntnisse. Im Übrigen gelten die Bestimmungen der separaten, vom AN zu unterzeichnenden, <i>Geheimhaltungspflichtungserklärung</i> .
Anl. 17 - 6	In dieser Anlage sind die Sicherheitsanforderungen aufgeführt, die der AN, wenn nicht anders angegeben oder zwischen den <i>Parteien</i> vereinbart, bei allen <i>Services</i> und Aktivitäten vom <i>Anfangsdatum</i> des <i>Vertrages</i> an, erfüllen bzw. einhalten wird.
Anl. 17 - 7	Der AN räumt MAN das jederzeit auszuübende Recht ein, nach vorheriger Anmeldung sämtliche Daten zu Geschäftsvorfällen zwischen MAN und dem AN bei dem AN einzusehen und zu überprüfen sowie die technischen und organisatorischen Maßnahmen zur Informationssicherheit zu überprüfen; MAN oder von MAN beauftragte Dritte dürfen hierzu bei Informationssicherheitsaudits die Räume des AN während der üblichen Geschäftszeiten betreten. Wenn Verstöße gegen die Vereinbarungen der jeweiligen Beauftragung und/oder die Informationssicherheitsrichtlinien festgestellt werden, trägt hierbei der AN die Kosten der Überprüfung und die Umsetzung risikomindernder Maßnahmen, es sei denn die Verstöße beruhen nicht auf einem Verschulden des AN.

Ref #	
Anl. 17 - 8	<p>Für die Erbringung von ausgelagerten IT Diensten durch einen externen Dienstleister, die in das interne Kontrollsystem der MAN fallen (IFR Systeme), sind Kontrollen zum IT Outsourcing vorgesehen.</p> <p>Hierzu ist vom AN jährlich, ein unabhängiger Auditor zu beauftragen, der den mit der Leistung verbundenen Kontrollrahmen überprüft und in einem ISAE 3402 Bericht zusammenzufasst.</p> <p>In Abhängigkeit der erbrachten IT Dienstleistung kann der Bericht in mehrere Teile gefasst sein:</p> <ol style="list-style-type: none"> <li>1. ISAE 3402 Type 2 Report –Basic Infrastructure Services System provided from the datacentres in Scope</li> <li>2. ISAE 3402 Type 2 Add-on Report – Database and Middleware Systems for ICFR relevant applications</li> </ol>
Anl. 17 - 9	<p>Die MAN wird dem AN bei Beauftragung und während der <i>Vertragslaufzeit</i> „Zugriff“ auf die jeweils aktuellen Dokumente der MAN Sicherheitsleitlinien sowie relevanter Regelungen und Anweisungen des Volkswagen Konzerns gewähren. Grundsätzlich gültig ist das Regelwerk zur Informationssicherheit der MAN Marke (<b>Anhang 17-A (Schutz- und Sicherheitsverfahren und Policy Pack)</b>). Die Regelungen der Volkswagen Gruppe sind dort gültig, wo keine explizite Regelung der MAN vorliegt.</p>
Anl. 17 - 10	<p>Im Falle von Unterbeauftragungen, des an MAN erbrachten Services, stellt der AN sicher, dass die hier beschriebenen Anforderungen in gleicher Weise an den Untertierlieferanten gestellt werden.</p> <p>Zudem stellt der AN sicher, dass MAN das in 17-7 beschriebene Prüfrecht auch beim Untertierlieferanten eingeräumt wird.</p>
Anl. 17 - 11	<p>Im Falle eines vermuteten Verstoßes gegen die Informationsschutzziele oder einer Beeinträchtigung der vom Auftragnehmer ergriffenen IT-Sicherheitsmaßnahmen, die sich auf die Erbringung der vertraglichen Leistungen auswirken können, informiert der Auftragnehmer das Cyber Defense Center der MAN (<a href="mailto:mtb-cdc@man.eu">mtb-cdc@man.eu</a>) unverzüglich und berichtet fortlaufend über die Aktivitäten zur Behebung des Vorfalls. Darüber hinaus wird der Auftragnehmer MAN in angemessenem Umfang bei der Schadensermittlung, -minimierung und -beseitigung unterstützen.</p>
	<p>Die folgenden Anhänge sind Bestandteil dieser Anlage 17:</p>
Anl. 17 - 12	<p><b>Anhang 17-A (Schutz- und Sicherheitsverfahren) und (Policy Pack)</b> enthält:</p> <p>Die organisatorischen Anweisungen beinhalten bestehende Richtlinien zur Informationssicherheit (Datenschutz und Datensicherheit) der MAN Marke.</p>

Ref #	
Anl. 17 - 13	<p><b>Auftragsverarbeitung:</b> Informationsverarbeitung im Auftrag liegt vor, wenn die Leistung des AN im Schwerpunkt mit der Verarbeitung von Informationen der MAN zu tun hat.</p> <p>Der AN muss durch eine entsprechende Zertifizierung die Eignung zur sicheren Informationsverarbeitung nachweisen.</p> <p>Werden durch den AN Informationen im Auftrag der MAN verarbeitet, die einen hohen oder sehr hohen Schutzbedarf und/oder Verfügbarkeit aufweisen, so ist eine <b>TISAX Zertifizierung</b> mit dem entsprechenden TISAX Label und Assessment Level 2, als minimum, nachzuweisen.</p> <p>In Abhängigkeit von der Serviceerbringung kann eine <b>ISO 27001 Zertifizierung</b> und deren Erweiterungen (für Cloud Services, Privacy System Management) über den Geltungsbereich, der alle Auftragsverarbeitungsaktivitäten beinhaltet, inklusive das Statement of Applicability (SoA) ebenfalls die Eignung bescheinigen.</p> <p>Zum Status über relevanter Informationssicherheitszertifizierungen, füllen Sie bitte <b>Anhang 17-G Zertifizierungsanforderungen Checkliste</b> aus.</p> <p>Falls der AN keine gültige Informationssicherheitszertifizierung nachweisen kann, so kann ein Vertragsverhältnis nur dann eingegangen werden, wenn sich der AN zu einer <b>TISAX Zertifizierung</b> innerhalb der nächsten neun Monate nach Vertragsbeginn, verpflichtet. Zudem ist vom AN eine <b>Gap Analyse</b> nach der TISAX Methodik VDA ISA einschließlich eines Aktionsplans zur Erreichung der Zertifizierungsstufe im geplanten Zeitrahmen bereitzustellen.</p>
Anl. 17 - 14	<p><b>Der Auftragsdatenverarbeitungsvertrag</b> beschreibt die Vorgaben der MAN zum Datenschutz der Auftragsdatenverarbeitung. Der Entwurf zur Auftragsdatenverarbeitungsvereinbarung dient zunächst nur zur Ansicht.</p> <p>Die relevanten und gültigen Versionen des Dokumentes (AVV mit Externen mit SCC, AVV mit Externen ohne SCC) sind zu finden unter: <a href="https://www.vwgroup-supply.com">https://www.vwgroup-supply.com</a>.</p> <p>Eine unterschriebene Version ist noch nicht bei Angebotsabgabe einzureichen und wird erst im Zuge einer Vertragsunterzeichnung berücksichtigt.</p>
Anl. 17 - 15	<p><b>Anhang 17-H (Sorgfaltspflicht für Informationssicherheit bei Partnern, Dienstleistern und Lieferanten)</b> umreißt Anforderungen der MAN Marke zur Sicherstellung einer ausreichenden Verfügbarkeit und Leistung bei der Bereitstellung von Produkten und Dienstleistungen, indem aktuelle Bedrohungen der Cybersicherheit berücksichtigt werden müssen und angemessen darauf reagiert wird.</p>